



# 松翰科技股份有限公司

## 資通安全風險及因應措施

### 一、資通安全風險管理架構

公司配有「資通安全小組」由資訊單位最高主管擔任召集人，並設置資安專責主管及資安專責人員，負責資通安全之管理、規劃、督導、執行等項目，其包含：制訂並定期檢討資安政策，建立資安事件通報與應變機制，持續深化防衛能力及加強同仁資通安全意識等項目，並每年定期向董事會報告；最近期向董事會報告日為 113.11.8。

### 二、資通安全政策

公司資通安全政策重點如下：

- 1.參考國際資安標準並遵守國內外資通安全法規，定期修訂最新資通安全規範。
- 2.與外部資安專家團隊合作，早期發現並防止資安威脅。
- 3.建立多層次防禦架構，加強防禦縱深。
- 4.強化資安專業能力與人力，強化內部資安規畫與事件分析處理能力。
- 5.持續資安教育宣導及災難復原演練。

### 三、資通安全管理方案

公司已採取或導入之具體管理方案如下：

- 1.新世代防火牆與入侵偵測系統
- 2.端點防毒與系統漏洞定期修補
- 3.郵件及網路多層次防毒防駭機制與聯防系統
- 4.網站弱點定期掃描與修正
- 5.資料定期備份與還原機制
- 6.定期舉行同仁資安宣導並測驗
- 7.定期社交工程防禦演練
- 8.建立資安事件分析監控及處理機制
- 9.加入資安聯盟以取得最新資安情資
- 10.每周進行[資安風險與因應措施]討論會議

公司強化措施以因應可能之駭客入侵，勒索病毒與 DDOS/APT 攻擊，持續關注外部資安事件，吸收新知強化資安控管，持續建立多層次防護及資安事件處理機制，加強宣導資通安全意識以因應日新月異的網路攻擊行為。另外公司機敏資料若須交付予廠商與客戶時，皆會要求簽訂保密合約，規範其保密義務。

### 四、投入資通安全管理之資源

113 年度公司已投入資通安全管理之資源如下：

- 1.資安教育訓練：完成全員工教育訓練與問卷 2 次。
- 2.社交工程演練：實施郵件釣魚演練 4 次，模擬攻擊情境並將點擊釣魚連結同仁進行教育訓練。
- 3.用於[資通安全]相關軟硬體經費逾新台幣 5 百萬元以上。